FRC GAS HUB PARTICIPANT USER GUIDE

PREPARED BY:	IMT - Gas Market Applications
FOR:	Gas Market Participants
DOCUMENT NO:	
VERSION NO:	7.0
EFFECTIVE DATE:	13 August 2009
ENTER STATUS:	Active

Version Control

VERSION NUMBER	CHANGES MADE	AUTHOR	DATE OF CHANGE
1.0	First draft		
2.0	Modified list of allowable ports for connectivity, following change to firewall rules. Allowable ports now in range of 5318 – 5330 inclusive, instead of 5318 – 5320 inclusive.	Darren Field	4.1.2005
3.0	Modified to include changes resulting from synchronising the FRC Relay Notification with Electricity B2b Notifications	Bert Naik	7.3.2007
4.0	Elaborated on the Cutover steps	Bert Naik	18.9.2007
5.0	Included the section on Industry Outage Window	Bert Naik	23.10.2007
6.0	Changed e-mail addresses	Jim Callaghan	12.02.2009
7.0	AEMO adoption	Bert Naik	13.08.2009

Table of Contents

1. Introduction 7

1.1 Audience 7

1.2 Acronyms 7

2. Overview 8

2.1 Stakeholders 8

2.2 Participant ID 9

2.3 Topology 9

2.4 Environments 10

2.5 Security 11

2.6 Administration 12

2.7 Provided Gateway 12

3. Entry Procedures 12

3.1 Network 12

3.2 Hub Connectivity 12

3.3 Participant Gateway Connectivity 13

3.4 Responders 13

3.5 Registration 14

3.6 Certification 15

3.7 Activation 15

4. Production 15

4.1 Support 15

4.2 Industry Outage Window 16

4.3 System Notifications 16

4.4 Transactions Log 17

4.5 Dispute Resolution 17

4.6 Security 17

4.7 Disaster Recovery and Business Continuity 18

Appendix A Responder User Interface 19

A.1 Certification 19
A.1.1 To perform an FRC certification 19
A.1.1.1 Using the Certification <Role> window 20
A.1.1.1.1 To select transactions on the Certification Role window 22
A.1.1.1.2 To clear all selected transactions in Certification Role window 23
A.1.1.1.3 To return to the Welcome window 23
A.1.1.2 Using the Confirmation window 23
A.1.1.2.1 To schedule a date and time for the certification transactions 24
A.1.1.2.2 To change the participant ID 25
A.1.1.2.3 To receive a summary report 25
A.1.1.2.4 To include specific data in the transactions you receive 25
A.1.1.3 Using the sandpit 26
A.1.1.3.1 To access the sandpit environment 26
A.2 Sending and validating aseXML 26
A.2.1 Sending XML 26
A.2.1.1 To send an aseXML document 27
A.2.2 Validating XML 27
A.2.2.1 To validate an aseXML document 27
A.2.2.2 The results of validating an aseXML document 28
A.2.2.2.1 Errors due to missing or invalid elements 29
A.2.2.2.2 Errors due to badly formed aseXML 30
A.3 Viewing transaction details 30
A.3.1 To access Web Manager on the production hub: 31
A.3.1.1 To search for a transaction 31
A.3.1.1.1 Fields in the search window 31
A.3.1.1.2 Wildcard characters 33
A.3.1.2 The document listing 33
A.3.1.2.1 To view document details 34
A.3.1.2.2 Viewing the Activity Log 34
A.3.1.2.3 Viewing the message content 35
A.4 System Notifications 35
A.4.1 The Notifications Window 35

A.4.1.1 To Send a Notification 36
A.4.2 Secondary Notification Method 38
A.4.2.1 To send via secondary method 39
Appendix B Troubleshooting Guide 40
Appendix C Disaster Recovery Provisions 41
C.1 Introduction 41
C.2 Overview 41
C.3 Disaster Scenarios 43
C.4 Cutover 46

Table of Figures

Figure 1 Production environment topology 10
Figure 2 Test environment topology showing responders 11
Figure 3: The Certification Role Window for a VICGAS retailer using schema version r9 22
Figure 4 The confirmation window 24
Figure 5 The send asexml document window 26
Figure 6 The validate asexml document window 27
Figure 7 validation results frame 28
Figure 8 Error when an item is missing from the xml 29
Figure 9 Error when an attribute is missing from the asexml 30
Figure 10 Error when a data element is too long in the asexml 30
Figure 11 Error when data has the wrong data type 30
Figure 12 The validation results from badly formed asexml 30
Figure 13 The web manager interface showing the transactions window 31
Figure 14 The search criteria window 32
Figure 15 Document listing 33
Figure 16 The document details window 34
Figure 17 The activity log window 34
Figure 18 Activity log entry of type 'error' 34
Figure 19 View document part contents window 35
Figure 20 The e-mail notifications window 36
Figure 21 Notification e-mail format 39
Figure 22 Troubleshooting contact guide 40

1. Introduction

This document contains information for participants in Australian Energy Markets to connect to, and use, the FRC Hub infrastructure put in place to accommodate the VicGas and SAWA Gas markets.

The document provides an overview of the system, and specific information for participants who wish to initiate a connection to the hub in order to operate in the relevant markets. The document also contains a number of appendices with detailed instructions on the use of certain features of the FRC system.

The document does not provide business, functional or technical information specific to any of the markets that use the hub for communication. This information is provided in business process documents, and functional and technical specifications supplied by the Market Operator of the market in which a participant wishes to operate. Contact the relevant Market Operator to obtain copies of these documents.

1.1 Audience

The document is targeted at actual and potential users of the FRC Hub environment with specific emphasis on the following roles:

Business Owners – May use the document to gain an understanding of the FRC Hub system in order to determine the business requirements of the system.

Project Managers – May use the document to determine the necessary planning that a participant or market operator must undertake in order to incorporate the FRC Hub in a market FRC implementation.

System Architects – May use the document to identify the architectural requirements of systems and processes necessary to operate in the FRC Hub environment.

Technical Developers – May use the document to identify the technical requirements, specifications and protocols necessary for a participants IT system to interact with the FRC Hub

1.2 Acronyms

ACRONYM	DESCRIPTION
aseXML	A Standard for Energy Transactions in XML. XML schema designed to accommodate the necessary transactions required to operate the energy markets
B2B	Business to Business. Interactions between two or more independent business participants.
CSR	Certificate Signing Request.
ebXML	Electronic Business XML. Protocol designed to facilitate B2B interactions.
FBS3	Hostname of the Test server

ACRONYM	DESCRIPTION
FBS6	Hostname of the Production DR server
FBS7	Hostname of the Production server
FRC	Full Retail Contestability
HTTP	Hyper Text Transfer Protocol
HTTP/S	Hyper Text Transfer Protocol/ Secure. HTTP using SSL for secure communications over the internet
ISP	Internet Service Provider
Market Operator	The entity that manages the operations of a specific gas market.
NEM	National Electricity Market
AEMO	Australian Energy Market Operator Ltd
REMCo	Retail Energy Market Company. Market Operator of the gas markets in SAWA
SAWA	South Australian and Western Australian Gas Markets
SSL	Secure Sockets Layer. Provides for encrypted transmission of documents over the internet and authentication using x509 certificates
URL	Universal Resource Locator
VicGas	Victorian Gas Market

2. Overview

The AEMO Gas FRC infrastructure enables participants to send business transactions over common network, message and transaction protocols. Business transactions are sent as aseXML documents carried as payloads inside ebXML message envelopes and transmitted over HTTP/S.

aseXML controls all business transaction functions, such as identification, timing, acknowledgment, transaction duplicate handling, etc. aseXML documents are generally handled by individual business back end systems.

ebXML controls message level functions such as reliable delivery, once-and-only-once delivery, message time-to-live, message integrity, non-repudiation, etc. ebXML messaging is generally handled via a single ebXML gateway, through which all aseXML transactions are routed. The hub currently supports ebXML v1.0 only.

HTTP/S controls network level delivery, network encryption, etc. HTTP/S enables messages to be sent securely over the internet, VPN or an agreed WAN/LAN network.

2.1 Stakeholders

The following are stakeholders in the hub and related infrastructure and are responsible in some way for administration, management and operations.

- **AEMO**. The current owner of the Hub and related infrastructure, and is responsible for administration, support, maintenance and future planning
- **Telehouser** The telehouser of the hub, and is responsible for the physical equipment and network, and day to day operations. The current telehouser is Hansens Technologies.
- **Gas Market Development** Section of AEMO that is responsible for the management of participants in AEMO market
- **REMCo** The SAWA Market Operator, and is responsible for the management of participants in that market
- **Participants** All entities who connect a gateway to the hub in order to send messages to another entity. Includes Distributions Businesses/Network Operators, Retailers/Users, and Market Operators.

2.2 Participant ID

A Participant Id is used in both the aseXML document and ebXML message to identify the sender and recipient of the message/transaction. Participant Ids in the VicGas, SAWA Gas and NEM markets are alpha-numeric, and no more than 10 characters in length. Both markets have identified a number of Participant Ids, including some that are not yet in use.

In the FRC infrastructure each Participant Id resolves to a URL to which the Hub will direct all messages, in other words an ebXML gateway. Therefore, new entrants to the hub infrastructure will need to ensure that their Participant Id does not conflict with any that have already been assigned by other markets.

2.3 Topology

The FRC infrastructure operates as a Hub and Spoke topology. Each participant, whilst needing to know the Participant Id of all other participants in the applicable market, need only set up a connection to the FRC Hub in order to be able to participate in the market. The hub routes messages to the desired recipient based the applicable architectural documents for the market.

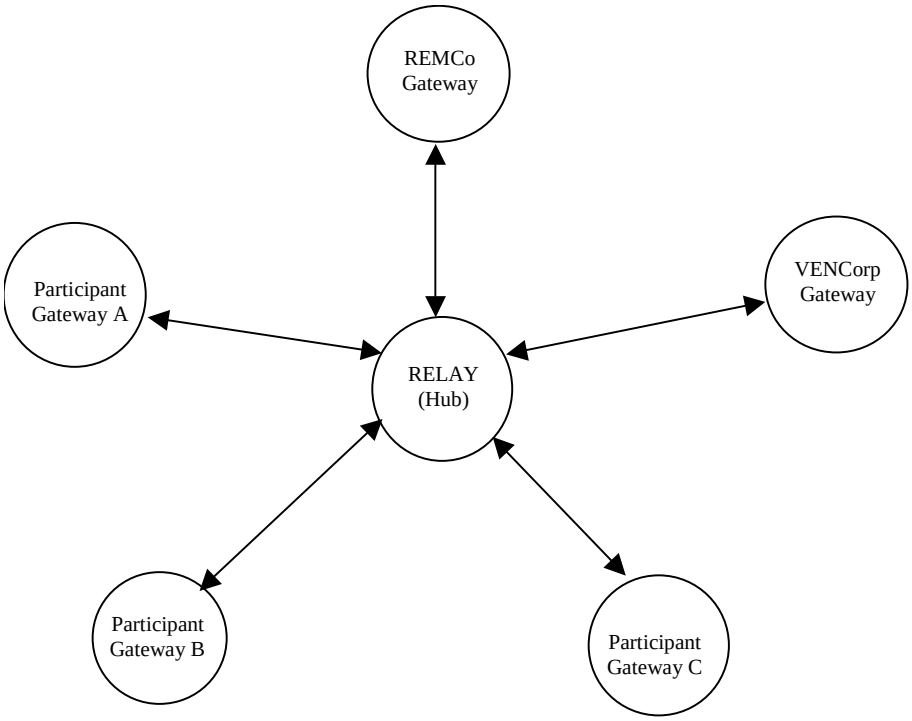


Figure 1 Production environment topology

Participant gateways are responsible for all end-to-end ebXML message functions such as reliable delivery, time-to-live, once-and-only-once delivery, etc. The hub is responsible for digital signature validation, re-signing using it's own certificate, and routing messages to the correct recipient.

2.4 Environments

The infrastructure consists of a test/certification environment and a production environment. Participants initially connect to the test environment in order to test their systems and certify them for use within the production environment. Following successful certification a participant can then connect to the production hub and exchange ebXML messages containing aseXML payloads with other participants in accordance with the various business, architectural and technical documents applicable to the relevant market.

Each hub – test/production – is configured individually. Therefore, a participant may use the same Participant Id, but with a different URL, on each hub, thus enabling different test/production gateways to be used. In addition, a participant may negotiate more than one Participant Id for the test hub to enable more than one gateway to be connected.

The test/certification environment contains, along with the Test Hub, two responders that act as mock gateways and are used for testing and certification. These responders have Participant Ids of FBSTEST (Sandpit) and FBS (Certify). Therefore, in a participant's test environment these two Participant Ids need to be accepted as valid Ids.

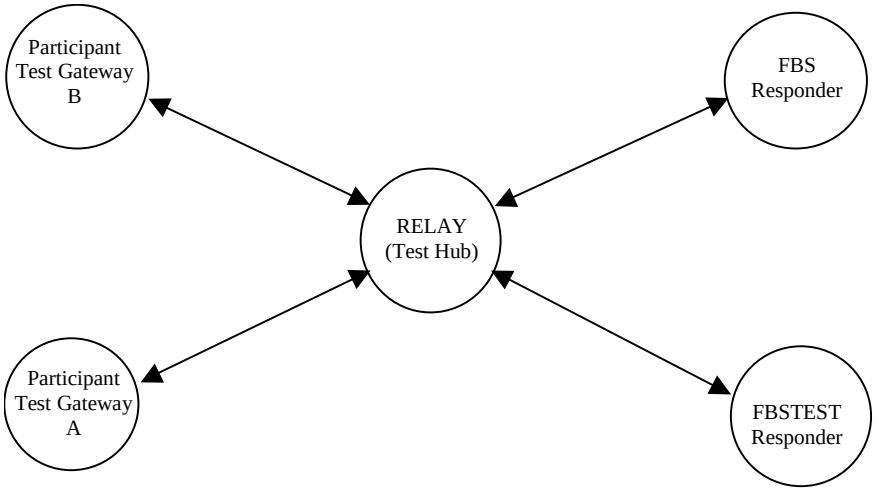


Figure 2 Test environment topology showing responders

FBSTEST may be used by a participant at any time to test functionality of their gateway. FBS may only be used for official certification testing in accordance with section 3.6.

2.5 Security

All communications between the FRC Hub and a participant's gateway are carried out using HTTP/S over SSL. SSL encryption is controlled using public/private key pairs, with a different key pair required to connect to each hub (Test/Production). In addition, ebXML messages are digitally signed using the same key pairs to guarantee data integrity and message non-repudiation.

Each participant must create/obtain a private key and a Certificate Signing Request (CSR). Two private keys/CSRs must be generated – one for testing and one for production. The CSRs are forwarded to FBS Administration, who will arrange for the production of Public Keys verified by the FBS Administration Certificate Authority (CA). The Public Keys will be returned to the participant along with the FBSAdmin CA Certificate, and the Public Keys for the Test Hub and the Production Hub (as applicable). FBS Administration will also retain copies of the generated Public Keys for application to the applicable hubs.

Each hub, as well as the certification responders, provide a browser interface that enables a participant to view messages that have been generated by the responders and routed through the hub. The Test environment allows connection to this interface using HTTP by supplying a username and password. The username will be the participant's Participant Id, and the password will be provided on registration. To connect with a browser to the Production Hub, or the Test Hub or Responders over HTTP/S, a participant must convert their Private Key to a PKCS#12 format and install this on their client machine.

If a participant does not currently have access to software to create keys, a suitable application is available for download free from http://www.openssl.org.

2.6 Administration

The hubs are currently administered by AEMO. The name of the administration section is FBS Administration or FBSAdmin. To contact FBSAdmin call either 03 9648 8616 or 03 9684 8619, or e-mail fbsadmin@AEMO.com.au

This is a technical administration only (i.e. hub connectivity, message throughput, etc). For issues relating to market operations (i.e. customer transfers, B2B issues) contact the applicable participant or market operator directly.

2.7 Provided Gateway

The FRC Hub uses webMethods Integration Server as the application. The licence for this application also provides for the supply of webMethods software to participants to use as a gateway in the FRC Hub environment. The software can be installed and configured as an ebXML gateway out of the box, with services also provided to help integration with participants back end systems. There are restrictions on the usage of this gateway but it is free of charge.

Contact FBSAdmin if you wish to use webMethods as your gateway.

3. Entry Procedures

3.1 Network

Participants can connect to the hubs via the internet or through the Victorian Gas Industry Network (VGIN).

If connecting using the VGIN a participant will need to:

- arrange/ensure VGIN connectivity arrangements with the telehouser
- arrange firewall access to FBS3 (Test) and FBS7/FBS6 (Prod) with the telehouser

If connecting over the internet then no more should need to be done other than private ISP arrangements, but it is wise to confirm routing and networking with the telehouser.

It is recommended that both paths be arranged in case of failure of one of the access methods.

Unfortunately there is no shortcut method for determining successful connectivity at the network level. Only the HTTP/HTTPS ports are made available, so ICMP things like Ping and TraceRoute cannot be used. Once ports are set up, FBSAdmin can work with a participant using HTTP/S to ensure connectivity.

3.2 Hub Connectivity

To connect a gateway to hub use the following URLs:

- Production Hub – https://www.frchub.net:5319/invoke/relay/inbound
- Test Hub – https://test.frchub.net:5319/invoke/relay/inbound

In addition, to connect to the browser interface of either the hubs or the responders use the following URLs:

- Production Hub - https://www.frchub.net:5319/WmTNWeb
- Test Hub
  - Over HTTP/S - https://test.frchub.net:5319/WmTNWeb
  - Over HTTP – http://test.frchub.net:5318/WmTNWeb
- Sandpit (FBSTEST)
  - Over HTTP/S – https://test.frchub.net:6319/WmTNWeb
  - Over HTTP – http://test.frchub.net:6318/WmTNWeb
- Certify (FBS)
  - Over HTTP/S – https://test.frchub.net:7319/WmTNWeb
  - Over HTTP – http://test.frchub.net:7318/WmTNWeb

3.3 Participant Gateway Connectivity

Participants will define their own URL, either by IP address or DNS name, to use for their gateway. The only requirement for URLs is that they must use a port between 5318 and 5330, as these are the only ports enabled through the hubs firewall

All other ports are blocked by firewall rules and cannot be used.

3.4 Responders

The Responders are a part of the Test Hub infrastructure and are available for participant use. The functionality available to users is:

- aseXML validation – submit an aseXML document and have it validated against the aseXML schema
- aseXML message sending – submit an aseXML document and have it wrapped in ebXML and sent to the defined recipients test gateway.
- Certification – a number of screens to guide a participant through the certification process.
- System notifications (see section 4.3).

The above functionality is available through a browser interface. See Appendix A for instructions in the use of this functionality.

The Responders also function as a participant gateway if ebXML messages are sent to them via the Test Hub. In this instance the functionality available is as follows:

- ebXML messaging functions (acknowledgments, errors, etc)

- aseXML transaction validation and acknowledgment

To use the above functionality send an ebXML message containing an aseXML transaction, with the Receiver set to ‘FBSTEST’ or ‘FBS’, through the Test Hub. The Responder will receive the message and return an ebXML acknowledgment. The Responder will then validate the aseXML transaction and return an ebXML message containing an aseXML transaction acknowledgment.

3.5 Registration

In order to use the FRC Hub infrastructure a participant must first register with the Market Operator for the market in which they wish to operate. Contact the relevant Market Operatror for details on how to register in that market.

The Market Operator will contact FBSAdmin and provide the following participant information:

- Company Name
- Participant Id
- Nominated Contact Name
- Nominated Contact Phone Number
- Nominated Contact E-mail Address.

The Nominated Contact can then use the registration form, available from the AEMO website, to register on the applicable hub. To obtain the form, go to http://www.aemo.com.au, and select ‘Metering & Retail Development’ from the menu. The form is available under the heading ‘FRC Gas Hub’.

Instructions for completing the form are contained in the form. You will need to know the URL of your gateway and receiving service, as well as providing a contact name and number. If there are any questions contact FBSAdmin

Submit the form along with a CSR (see Section 2.5) to fbsadmin@aemo.com.au. You will receive certificates for access to the applicable hub, and a password if your request is to access the Test Hub and Responders.

The general sequence for hub registration is:

- Register for use on the Test Hub
- Activate on Test Hub and Responders
- Test using Sandpit (FBSTEST), bilateral tests, etc.
- Certify as required using Certify (FBS)
- Register for use on Prod Hub

- Activate on Prod Hub

3.6 Certification

Currently, all Market Operators require that participants pass certification before they are allowed access to the Production Hub. Each Market Operator has a Certification Process document that describes the necessary steps to be taken by participants in order to certify. Contact the relevant Market Operator to obtain a copy.

The certification process involves sending documents to, and receiving documents from, the Certification Responder (FBS). To support the process a browser based User Interface is available on the Responder. See Appendix A for instructions in the use of this interface.

Once certification is carried out FBSAdmin will review the transactions and acknowledgements that have been sent by the participant. A report will be created and forwarded to the participant and the relevant Market Operator. The Market Operator will review the report in accordance with that market's requirements and, if satisfied with the results, will notify FBSAdmin and the participant of successful certification.

Following successful certification FBSAdmin will create a profile on the Production Hub which, when activated, will enable the participant to sent production transactions within the applicable market.

3.7 Activation

In order to activate their profile on the Production Hub a participant must formally request this through the applicable Market Operator. Contact the relevant Market operator to determine their requirements for activation. At a minimum, for activation FBSAdmin need the following information:

- The date that you wish to become active in the Production environment
- The transactions that you intend to use

FBSAdmin will confirm that you are certified for the proposed transactions and activate your profile at the appropriate time.

4. Production

4.1 Support

The hub and infrastructure are supported 24x7. Level 1 support is currently supplied by the telehouser Helpdesk. All technical issues relating to the hub infrastructure should be directed to this Helpdesk in the first instance. They will determine whether the problem can be handled by the telehouser, or whether to escalate the issue to FBSAdmin.

AEMO Helpdesk is available during business hours to accept calls for administrative and functional issues regarding the hub application. AEMO Helpdesk will escalate all relevant issues to FBSAdmin for resolution.

FBSAdmin have staff on-call 24x7 should the need to escalate arise.

Each Market Operator has a Helpdesk to accept business related issues. Issues relating to individual participants should be directed to the relevant participants helpdesk.

See Appendix B for a troubleshooting guide with further information regarding contacts in the event of issues.

4.2 Industry Outage Window

The Hub and the related infrastructure may be unavailable for normal business during the scheduled Industry Outage Window of 4 hours on Sundays - starting at 10:00AM EST. This time may be utilised by the Hub Service Provider or the telehouser to apply any low-impact patches and fixes.

The Participants are advised not to schedule any batch jobs to send messages during this Window as well as for three hours preceding the Window. The reason for avoiding the batch jobs for three hours before the window is to minimise the risk for manual sending of messages in the event that the ebXML Acks from the recipients have not been received due to any problems in processing the message at the recipient gateways.

Hence, although the Industry Outage Window is effective between 10:00AM and 02:00PM (EST) on Sundays, the Participants are advised to avoid sending messages between 7:00AM and 02:00PM (EST).

However, it may be noted that the unavailability of the Hub/s during the Industry Outage Window is rare.

4.3 System Notifications

Participants have an obligation to broadcast certain information regarding their IT systems to all other participants in the markets. This is information such as planned and unplanned outages of gateways, performance issues and other information that a participant believes may assist in the smooth operation of the FRC B2B System.

A User Interface has been created on the Sandpit and Certify Responders for participants to use when sending these notifications. The interface takes a number of inputs from the user, and generates an e-mail that is sent out via a defined distribution list. The interface has been put in place to ensure a consistent format of message, so that recipients can automate processes based on the receipt of these notifications (i.e. send an SMS alert, etc).

The interface sends a message to a mailbox that has a distribution list assigned. Each participant who needs to receive notifications is able to assign one e-mail address to this distribution list. This address should not be a personal mailbox, but rather a company mailbox that, in turn, can distribute the notifications as the participant desires. In this way each participant can manage changes to internal notification distribution without constantly requiring changes to the main distribution list maintained by FBSAdmin. The mailbox is known as FRCRelay, and a participant provides the e-mail address as part of the registration process.

See section A.4 for instructions in the use of the notifications interface.

4.4 Transactions Log

Both the production and test hubs have a browser interface available to participants through which they may view their ebXML messages. From this interface you will be able to determine basic information about your messages, particularly whether a message was delivered successfully to the recipient or not.

See section A.3 for instructions in the use of this interface.

4.5 Dispute Resolution

ebXML message data on the Prod Hub is retained on line and available to participants as per section 4.4 for eight days. In addition, the data is retained in an archive for a period of seven years.

Using this data, FBSAdmin can provide resolution in the event of a dispute between participants over such things as message delivery, non-repudiation of message content, etc. If a participant requires data from an archive, they are to send a request to FBSAdmin. Either a date/time window or a specific ebXML MessageId is required to enable identification of the data.

4.6 Security

As stated in section 2.5 participant gateways connect to the Production Hub using HTTP/S and Public/Private key pairs. Participants are responsible at all times for the security of their private key. If the private key is compromised, the integrity of the authentication, encryption and non-repudiation functions of the FRC system cannot be guaranteed. If a participant believes their key may be compromised they must immediately:

- Notify FBSAdmin. Depending on the circumstances of the compromise, FBSAdmin may choose to disable the participants profile to stop receipt of messages.
- Generate a new Private Key and Certificate Signing Request (CSR)
- Send the CSR to FBSAdmin. FBSAdmin will arrange the creation of a new certificate and return this to the participant
- Immediately, if the profile has been disabled, or at an agreed time if not, FBSAdmin and the participant will change to the new certificate set.
- Notify all participants, either via FRCRelay (see section 4.3) or through the applicable working groups.

The private key of the hub is also at risk of compromise. If this occurs then all participants will be effected, as the hub's key set will need to be changed. FBSAdmin will carry out the following if compromise of the key is suspected.

- Notify all participants via FRCRelay (see section 4.3)

- Generate a new Private Key and Certificate
- Send the Certificate to all participants
- Notify all participants of a time that the new certificate is to be applied.
- At the agreed time, replace the certificates and work with participants to ensure connectivity is maintained.

4.7 Disaster Recovery and Business Continuity

In order to maintain Business Continuity, the FRC Hub environment consists of a Primary Site and a Disaster Recovery Site. Should an incident disable the Primary Site, or critical components within the Primary Site, control will be transferred to the DR Site. The actions necessary for both the participant and the hub provider to implement this transfer will vary, depending on the impact of the incident.

See Appendix C for details of the DR facilities and analysis of participant requirements to support these facilities.

Participants should also have a DR solution for their gateway in place. Provision is made in the registration process for an alternative URL to be recorded, if this is required as part of the solution.

Appendix A Responder User Interface

A.1 Certification

The purpose of certification is to verify that Gas Market participants can connect to the FRC Hub and then use it to send and receive messages and aseXML transactions. These messages and transactions must conform to the standards described in Participant Build Packs 2 and 3.

There are two types of certification transactions. These are:

- Technical transactions that establish a participant's ability to connect to the FRC Hub
- AseXML transactions that describe the business processes undertaken by a participant acting in a given market role

The following windows are a tool set to help you, as a participant, to successfully complete the FRC Certification Process. You nominate for which transactions you want certification, you schedule the execution time of the transactions you will receive, and you provide data for those transactions. For a first time certification, you nominate all the transactions that you need to send or receive across the FRC B2B System. You can then limit subsequent certifications to a subset of transactions.

Certification transactions are grouped by Market, aseXML Schema Version and Market Role. Once you select the appropriate Market, Schema Version and Market Role for your organization, a list of certifiable transactions for that role appears. From this list, you select transactions either individually or, for convenience, by Transaction Group. At any time, you can return to the main menu and so cancel any transactions you may have selected.

Once you have selected the transactions, then you can:

- Provide data to populate the transactions sent to you by the Certification Process.
- Choose to have transactions sent immediately or schedule them for sending at a later time

A.1.1 To perform an FRC certification

1. If you are using digital certificates, in the Address box of your browser, type https://test.frchub.net:7319/WmTNWeb.

   —or—

   In the address line of your browser, type http://test.frchub.net:7318/WmTNWeb and enter your Participant ID and Password (provided by FBS Admin when your organisation was registered for the FRC B2B System).

2. Log on to the Responder and from the menu, choose Certification.

3. Once you have read the Welcome window, click the ‘click here’ link.
4. The **Market and Schema Selection** window appears
5. Locate the market for which you wish to be certified and click the applicable schema version.
6. The **Gas Market Role Selection** window appears
7. Click the role that your organisation fulfils in the gas market - that is one of:
   (a) Retailer/User
   (b) Distributor/Network Operator
   (c) Market Operator
8. On the **Certification > <Role>** window, select the transactions you want certification for, scroll to the end of the window, and then click Continue. (See ‘Using the Certification <Role> window on page 20 for details.

Warning

Do not use the Back button in your browser to return to a previous window when using the certification system. AEMO cannot guarantee the resulting transaction status.

9. On the **Confirmation** window, set the execution time and any optional inputs required. If you want a confirmation e-mail make sure you enter an e-mail address. The system sends a summary of the certification process you have requested to the mailbox you nominate.
10. Scroll to the end of the window and click Confirm.
11. On the **Summary** window, check your details and if correct, click Submit.
12. The system displays a message to show that the service is completed. This may take some time if you are running the service immediately. If you scheduled the service to run in the future the final response should be almost immediate.

A.1.1.1 Using the Certification <Role> window

On the Certification Role window, you select the type of transaction you want to certify. You can certify that you are able to receive specific transactions from the responder, or you can choose to send transactions to the responder, and the system will validate these and confirm the result.

Transactions appear under those sent to your organisation by the responder, and those sent from your organisation to the responder. The transactions available are the ones pertaining

to the market, schema version and role you selected. There are many possible transactions. For your convenience, these transactions are grouped under Transaction Group headings. You can quickly select one or more of these headings to get all the transactions in that group. Alternatively, you can select individual transactions.

Note

Certification is a process between your gateway and the responder. No other participants are involved. Once you have certified your system for a particular transaction, in both directions, you can send messages to and receive messages from other participants through the hub.

If you select All, the responder will validate that your front-end system can both send and receive all allowable transactions for your role.

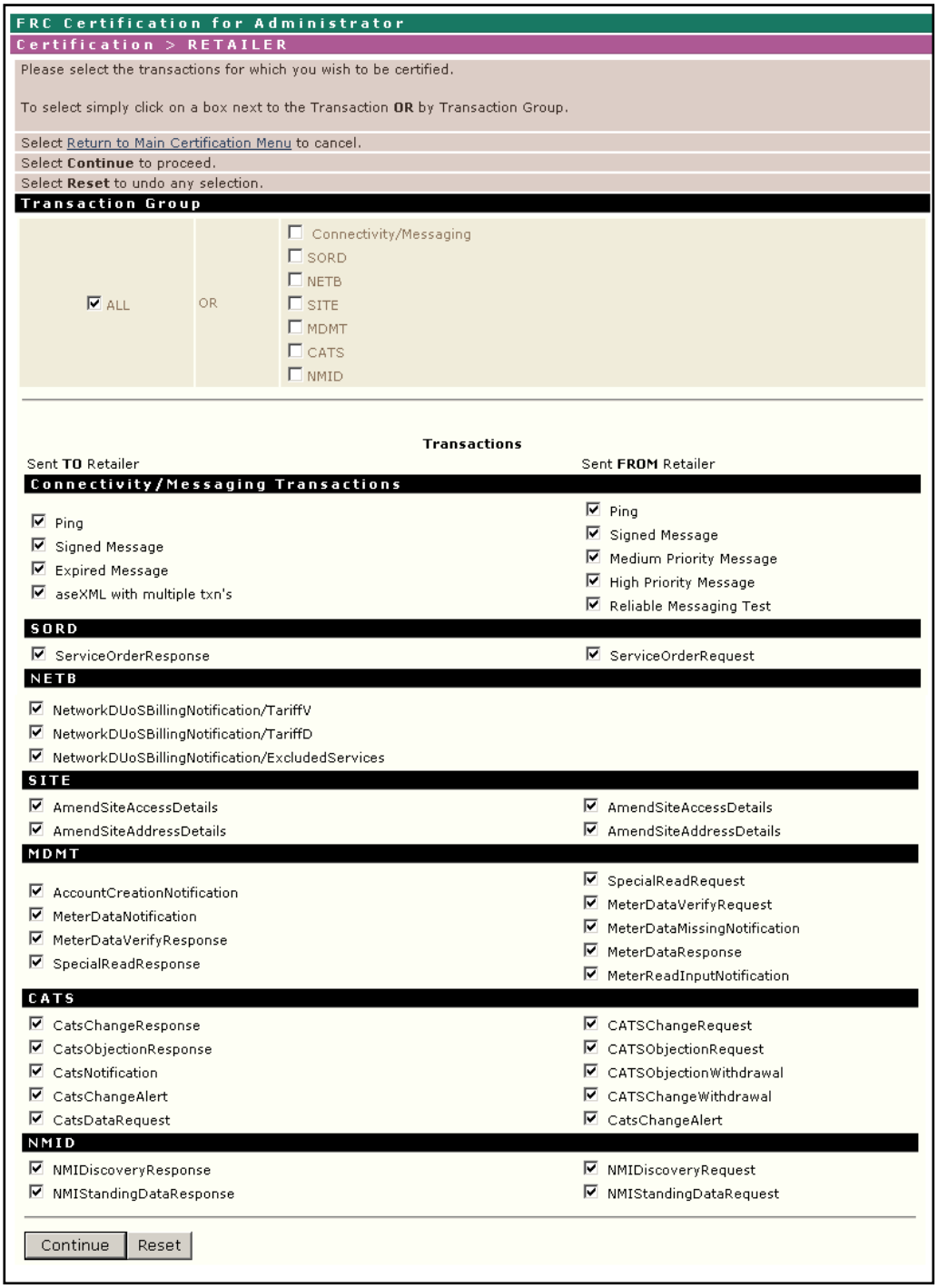


Figure 3: The Certification Role Window for a VICGAS retailer using schema version r9

A.1.1.2 To select transactions on the Certification Role window

1. If you want all of the transactions in a group, select one or more of the following checkboxes in the Transactions Group section,:

   (a) Connectivity/Messaging transactions group

   (b) SITE – Amend site details group

   (c) SORD – Service orders group

(d) NETB – Network DUoS billing notification group

(e) MDMT – Meter data group

(f) CATS – CATS transactions group

(g) NMID – MIRN data group

(h) CUST – Customer Details Group

Note

The number of groups available depends on the role, market and schema version you chose before you to entered this window.

2. If you want to select only some transactions, select the checkboxes next to those transactions. You can also select a transaction group and then clear the checkboxes for unwanted transactions in that group.
3. When you have completed your selections, scroll to the end of the window and click Confirm.

A.1.1.3 To clear all selected transactions in the Certification Role window

► Scroll to the end of the window and click Reset.

A.1.1.4 To return to the Welcome window

► Click the Return to Main Certification Menu link.

Warning

Do not use the Back button in your browser to return to a previous window when using the certification system. AEMO cannot guarantee the resulting transaction status.

A.1.1.5 Using the Confirmation window

On the confirmation window, you confirm your selection of transactions for certification, and, optionally, schedule the time of execution for those transactions. You can also provide data for those transactions that the Certification Process initiates and sends to you. The responder does not use data you enter in this window in any transactions that you initiate.

If you do not request a Schedule Date and Time, the responder sends transactions initiated by the Certification Process, immediately.

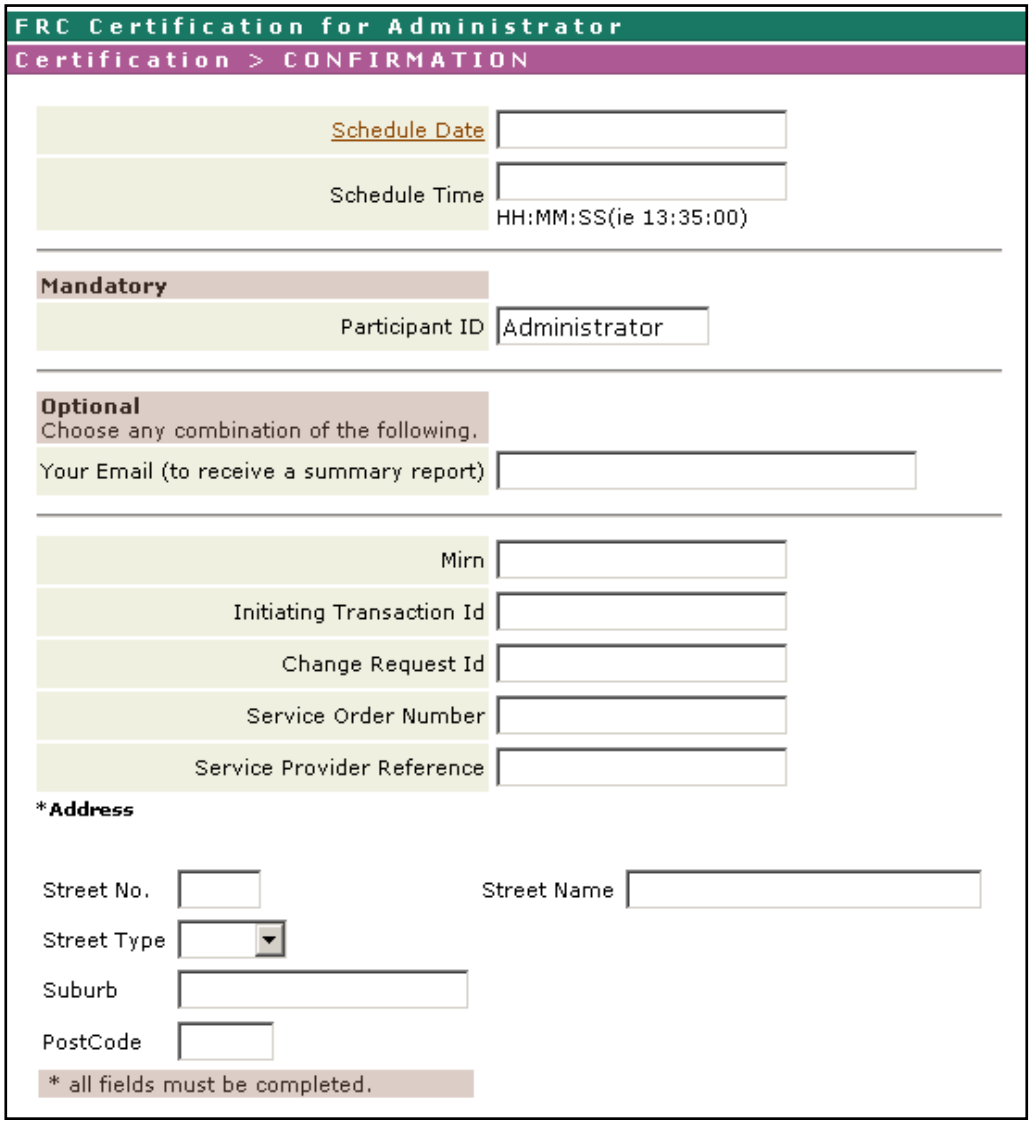


FIGURE 4 THE CONFIRMATION WINDOW

A.1.1.6 To schedule a date and time for the certification transactions

1. On the Confirmation window, click the Schedule Date link and pick a date from the calendar. Use the arrows either side of the month name and year to change these items. Select a date by clicking the day in the calendar. Click Set when you have finished.

Note

The date format used is the international format of Year/Month/Day. Thus, 21 July 2002 appears as 2002/07/21.

2. Type a time in the format HH:MM:SS. Note that if you enter a Date you must also enter a Time.

You should not schedule a date and time before the present. If you do, the responder will return an error to the screen on submission.

A.1.1.7 To change the participant ID

Note

The system must have a participant ID to whom to send the return transactions. This is normally the ID you used to log on. The responder inserts your log on ID as the Participant ID as a default. You can change this ID, if necessary.

- ► Type your new ID in the Participant ID box.

A.1.1.8 To receive a summary report

- ► Type a valid email address in the Your Email box. The responder sends a summary of your transaction request to this email address.

A.1.1.9 To include specific data in the transactions you receive

Note

You can request that the responder include specified data in the transactions it sends back to you. Only provide one set of input data per certification process. All responder-initiated transactions nominated by you and which contain the relevant data elements use the data you provide.

1. If required, type a valid entry for one or more of the following items:
   (a) MIRN
   (b) Initiating transaction ID
   (c) Change request ID
   (d) Service order number
   (e) Service provider reference
2. If you require a specific address in the return transaction, type valid address details in all of the address section boxes. You must complete all of the following:
   (a) Street number
   (b) Street name
   (c) Street type
   (d) Suburb
   (e) Postcode

A.1.1.10 Using the sandpit

The sandpit environment is a mirror of the certification environment. The sandpit is for participants to use when they wish to send messages through the FRC B2B System in a test environment. Participants can practise the certification processes in the sandpit before requesting formal certification via the certification user interface. The sandpit environment is on the pre-production FRC Hub with the certification environment. You access it in the same way as the certification environment but using different ports.

A.1.1.11 To access the sandpit environment

► If you are accessing the responder through a secure port using digital certificates, in your browser address box, type https://test.frchub.net:6319/WmTNWeb.

—or—

► If you are accessing the responder through a non-secure port using a user name and password, in your browser address box, type http://test.frchub.net:6318/WmTNWeb and then type your Participant ID and password.

A.2 Sending and validating aseXML

The FRC responder provides a facility to both send aseXML and to validate aseXML without sending.

A.2.1 Sending XML

To send an XML message, you use the Submit aseXML Document window. The Send aseXML utility wraps your aseXML in ebXML and sends it via the Test FRC Hub.

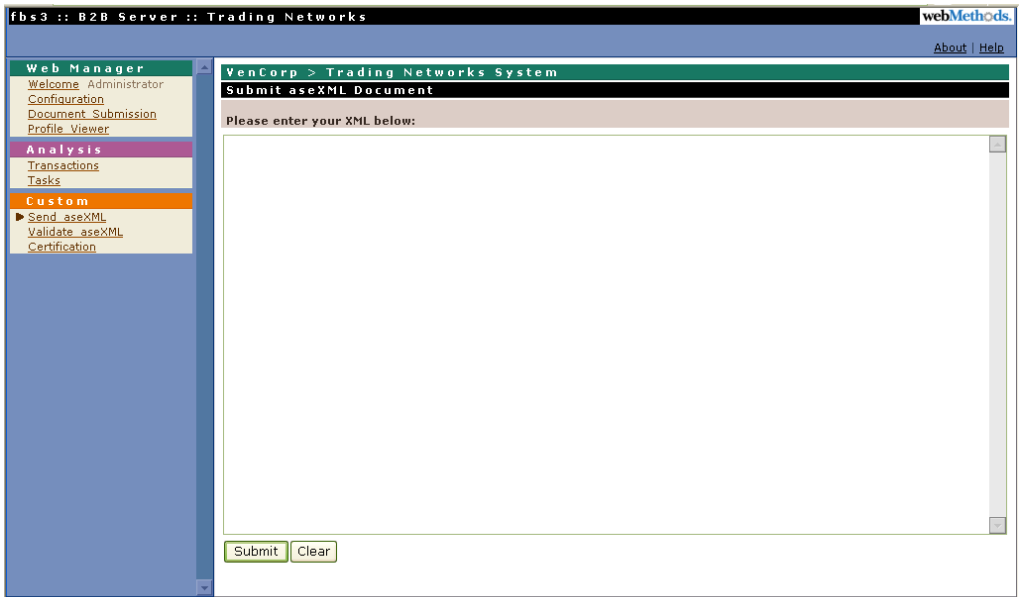


Figure 5 The send asexml document window

A.2.1.1 To send an aseXML document

1. From the Responder menu, choose Send aseXML.
2. In the Send aseXML Document window paste your XML in the space provided.

Note

The 'From' in your aseXML must match the Participant ID of the responder you are using. This is 'FBSTEST' for the Sandpit and 'FBS' for Certify.

3. Click Submit.

A.2.2 Validating XML

The FRC Responder provides you with a useful tool for validating your aseXML without sending it. Validation checks the structure of your aseXML data against the aseXML standards currently in use by the Victorian Gas Market. It does not check the validity of the actual data presented

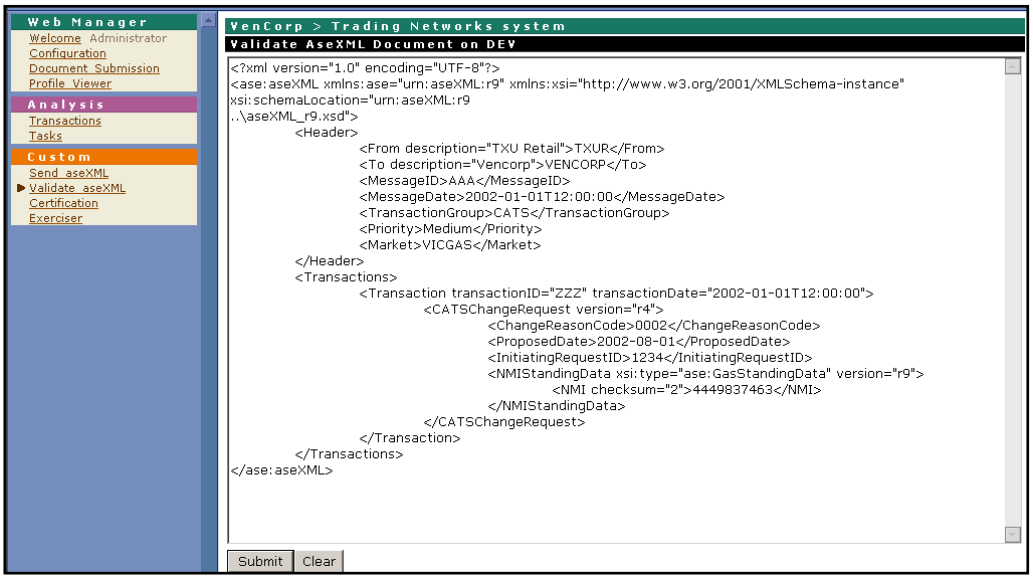


Figure 6 The validate asexml document window

A.2.2.1 To validate an aseXML document

1. From the Responder menu, choose Validate aseXML.
2. In the Validate aseXML Document window paste your XML in the space provided.
3. Click Submit.

Tip

You can use the Validate aseXML window as a simple editor. If validation fails, click Back to go back to your aseXML and make minor changes.

A.2.2.2 The results of validating an aseXML document

If the document is valid, when you submit it, the software returns a frame for the validation like the one shown below.

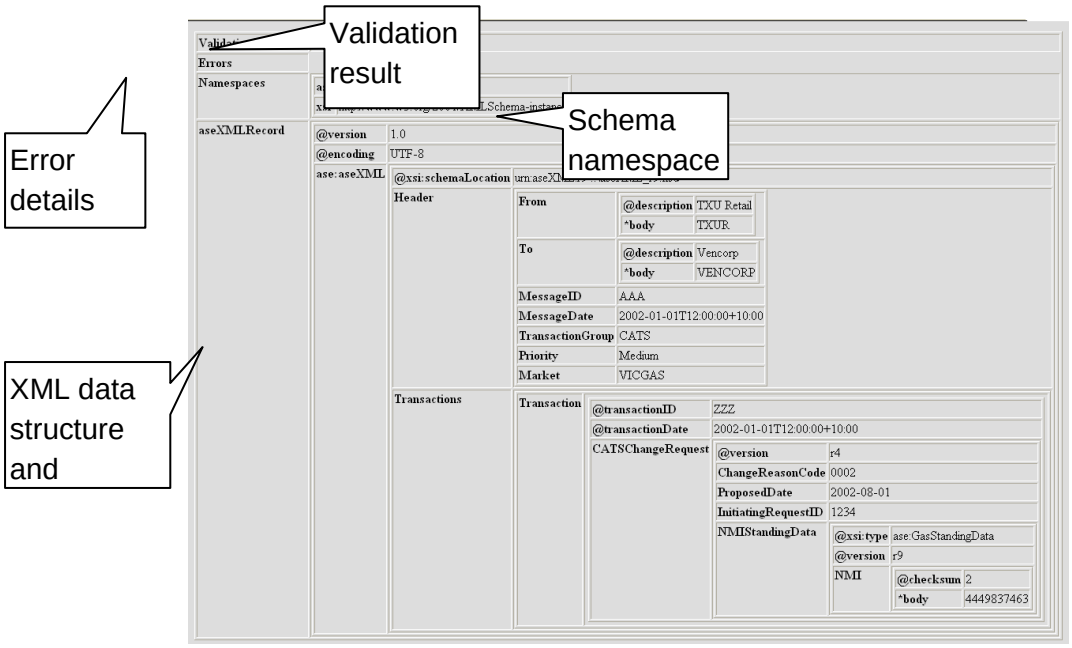


Figure 7 validation results frame

The validation results frame has four parts. Details of these parts appear in the following table.

Section	Comments
Result	Either True for a valid result or False for an invalid one.
Error details	This section shows the details of any errors that may have occurred.
Schema namespaces	The namespaces detected in the input document

Section	Comments
XML data structure	This section lays out the structure of the XML document in tabular form. Columns indicate the layers in the document. The first column represents the outermost layer, and so on. The tag names appear in bold text. An "@" before the tag name represents an attribute. The data elements between tags where attributes are present is represented where necessary by the form "*body". Each time, the data appears in non-bold text in the final column. By tracing across the columns, you can determine the path for a particular data element. For example, in the above figure, the tag ChangeReasonCode has the path: `/aseXML/Transactions/Transaction/CATSChangeRequest/ChangeReasonCode.`

Two types of error occur; those due to missing or invalid elements, and those due to badly formed aseXML.

A.2.2.3 Errors due to missing or invalid elements

If an element of the standard aseXML is missing, the validation returns a False result and the element is missing from the data structure section. Further details appear in the Error Details section.

For example, if the 'Transaction Group' line in the above aseXML is missing, the validation returns an error result like that shown below.

errorMessage	aseXML schema validation failure on payload. Path:/aseXML/Header/ Error message:[B2BCORE.0082.9009] Child element Priority {} at position 4 is unexpected

Figure 8 Error when an item is missing from the xml

The error message indicates that the validation did not expect to get a data item where it did. The Path Name tells you in which section of the aseXML the error occurred. In this case, it is in the Header section. The statement in the error message 'Priority at position 4' tells you that it has found the element Priority at the fifth line (counting starts from zero) where it expected some other element. The element normally above 'Priority' must therefore be missing.

Note

Where an element is optional, validating XML with this element missing produces a True result.

The following error occurs because an attribute is missing.

errorMessage	aseXML schema validation failure on payload. Path:/aseXML/Transactions/Transaction/CATSChangeRequest/@version Error message:[B2BCORE.0082.9007] Missing Attribute Information Item

Figure 9 Error when an attribute is missing from the asexml

In this case, it is the version attribute in the CatsChangeRequest tag.

If a data element is longer than the prescribed length, the following error occurs.

errorMessage	aseXML schema validation failure on payload. Path:/aseXML/Transactions/Transaction/CATSChangeRequest/ChangeReasonCode Error message:[B2BCORE.0082.9465] Value is longer than maximum length

Figure 10 Error when a data element is too long in the asexml

The following error occurred because the InitiatingRequestID was set as a string instead of a number.

errorMessage	aseXML schema validation failure on payload. Path:/aseXML/Transactions/Transaction/CATSChangeRequest/InitiatingRequestID Error message:[B2BCORE.0082.9447] Value does not conform to datatype

Figure 11 Error when data has the wrong data type

A.2.2.4 Errors due to badly formed aseXML

For badly formed aseXML, the Validation Results frame is a lot simpler. Because the Responder is unable to parse the xml, the aseXML contents will not be presented..

ValidationSuccessful	false
Errors	**errorMessage**: aseXML schema validation failure on payload. Path:General validation error. Error message:[B2BCORE.0082.9001] Error while parsing "[B2BCORE.0042.9327] Expecting </Header> got </ase:aseXML>"
Namespaces	**ase**: urn:aseXML:r9 **xsi**: http://www.w3.org/2001/XMLSchema-instance

Figure 12 The validation results from badly formed asexml

A.3 Viewing transaction details

The FRC hub runs on the webMethods Integration Server. The Web Manager user interface is an extension of the wM Integration Server and uses webMethods terminology on the screens that come as part of the base Web Manager interface. Because of this, the names used for some fields differ from the names commonly used in the gas industry. This section describes these differences as they appear in the Transaction Search area of Web Manager – the area likely to be used most by participants.

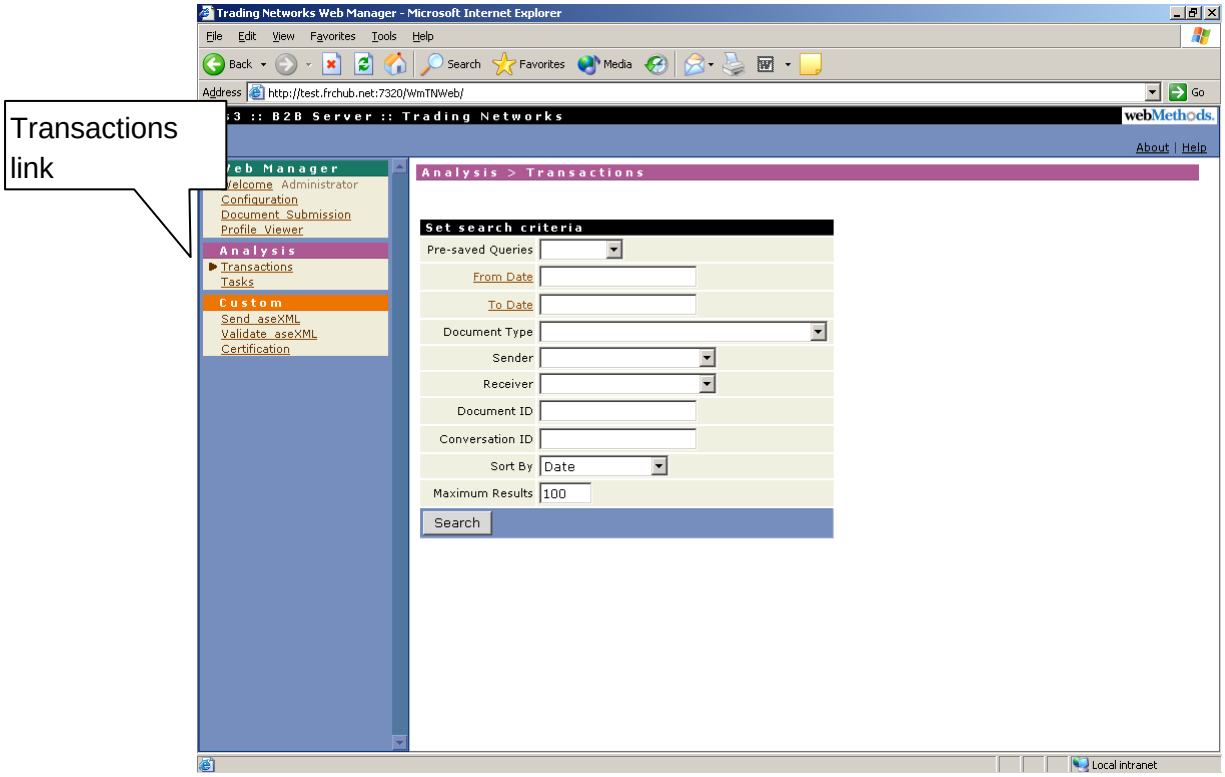


Figure 13 The web manager interface showing the transactions window

The Web Manager interface is available on both the production and test FRC hubs. The custom built features developed by AEMO, such as Certification, are only available on the test responder. The standard Web Manager screens, such as Transaction Analysis, are available on both.

This section discusses the screens presented under the Transactions link and highlights the differences between webMethods terminology and Gas FRC terminology.

A.3.1 To access Web Manager on the production hub:

► From the menu of Web Manager welcome screen, in the Analysis section, choose Transactions

A.3.1.1 To search for a transaction

1. From the Analysis menu, choose Transactions.
2. Enter suitable search criteria to narrow the search and click Search.
3. The hub lists all documents that fit your criteria.
4. Scroll down the list to find the document required.

A.3.1.2 Fields in the search window

Most of the terminology differences are in the Search Criteria window.

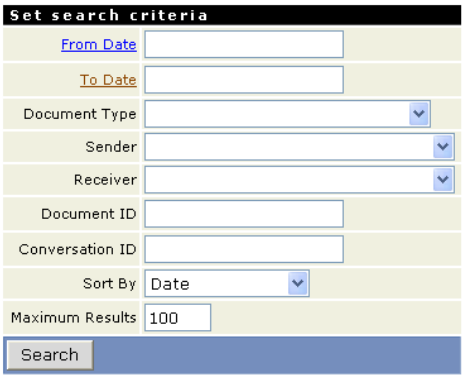


FIGURE 14 THE SEARCH CRITERIA WINDOW

The following table lists the fields in the Search Criteria window together with their equivalents. Note that all fields are optional.

Field	Comments
From Date	Set starting date for the listing
To Date	Set ending date for the listing
Document Type	Not relevant in this implementation
Sender	Not relevant in this implementation
Receiver	Not relevant in this implementation
Document ID	The ebXML message ID
Conversion ID	The ebXML conversation ID plus a number generated internally by WebMethods.
Sort By	Select from list
Maximum Results	Limits the number of transactions in the list

Note

Participants are only permitted to view documents as they transit between the participant gateway and the hub. Therefore the 'Sender' is always either the participant or the hub, as is the 'Receiver'. Because of this, if a 'Sender' is input the results will only display Sent messages, regardless of the Sender that is input. If a 'Receiver' is input the results will only display Received messages.

Field	Comments
Note	A Conversation ID is only recorded against messages that have been sent ‘From’ the participant. It is not recorded against the messages sent ‘To’ the participant.

A.3.1.3 Wildcard characters

For all fields where no list is available, the search accepts wildcard characters. Wildcards are:

_ (underscore) Single character

%(percent) Any group of characters

For example:

To search for a document ID containing the number ‘123’, use the form %123%.

A.3.1.4 The document listing

The hub lists all documents that fit your search criteria together with the basic details of those documents.

Received documents

Date	Type	From	To	DocID	Status
2004-06-21 11:45:01.557	ebXML v1.0 Default	FRC Test Hub	FBS Certify	REMCO 53afjj00vl2f7uqr0000024o	SendMessage:sent
2004-06-21 11:44:49.243	ebXML v1.0 Default	FRC Test Hub	FBS Certify	REMCO 53afjj00vl2f7ies0000024d	SendMessage:sent
2004-06-21 11:44:49.123	ebXML v1.0 Default	FRC Test Hub	FBS Certify	REMCO 53afjj00vl2f7in50000024g	SendMessage:sent
2004-06-21 11:44:40.13	ebXML v1.0 Default	FRC Test Hub	FBS Certify	REMCO 53afjj00vl2f7a2a00000244	SendMessage:sent

Sent documents

Date	Type	From	To	DocID	Status
2004-06-21 11:45:04.49	ebXML v1.0 Routing	FBS Certify	FRC Test Hub	FBS 5fu04300vl2e1ddh000007kf	MessageRouting
2004-06-21 11:44:51.947	ebXML v1.0 Routing	FBS Certify	FRC Test Hub	FBS 5fu04300vl2e116j000007kd	MessageRouting
2004-06-21 11:44:44.193	ebXML v1.0 Routing	FBS Certify	FRC Test Hub	FBS 5fu04300vl2e0ovv000007kb	MessageRouting
2004-06-21 11:44:42.913	ebXML v1.0 Routing	FBS Certify	FRC Test Hub	FBS 5fu04300vl2e0o7p000007k9	MessageRouting

FIGURE 15 DOCUMENT LISTING

The column headed DocID contains the MessageID for the ebXML document.

Messages are grouped into ‘Received’ (those messages received by the participants gateway), and ‘Sent’ (those sent by the participants gateway).

The Status of all messages received by the gateway should be ‘SendMessage:sent’. This indicates that the hub believes that the message was delivered successfully to the gateway. If the hub encountered an error attempting to send to the gateway the Status will be ‘SendMessage:err’. If you need to obtain further details regarding the specific error contact FBSAdmin.

The Status of all messages sent to the hub by the gateway should be 'MessageRouting'. If the hub encountered an error while processing the message (i.e. recipient not recognised, digital signature invalid, etc) the Status will be 'RouteMessage:err'. However, errors encountered while delivering the message to the intended recipient do not get reported on this screen. If you need to determine this information you need to view the Activity Log entries by following the directions below.

A.3.1.5 To view document details

► Click the date in the Date column.

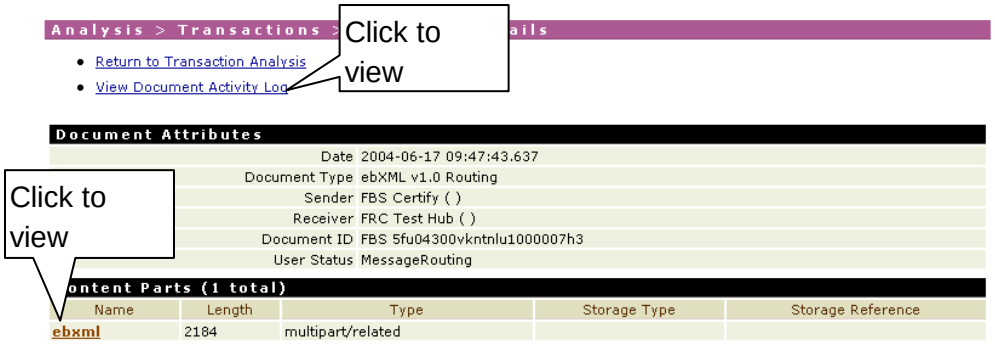


FIGURE 16 THE DOCUMENT DETAILS WINDOW

A.3.1.6 Viewing the Activity Log

To view the Activity Log for the message:

► Click the 'View Document Activity log' link

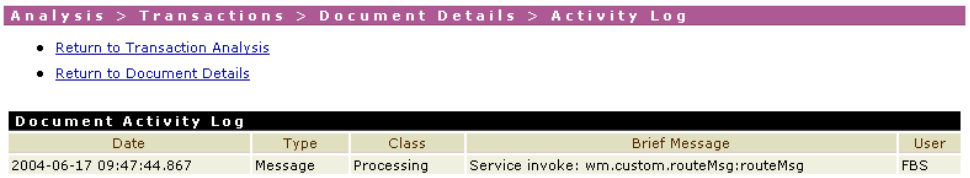


FIGURE 17 THE ACTIVITY LOG WINDOW

The 'Type' column indicates the type of log entry. If this is 'Message' the message was delivered successfully. If it is 'Error' the hub encountered an error while attempting to deliver the message.

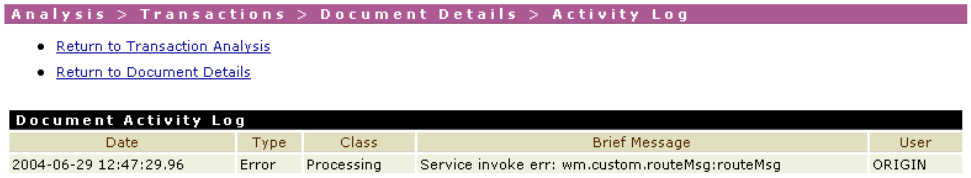


Figure 18 Activity log entry of type 'error'

Not all messages have an Activity Log entry. Messages received by the gateway that were successful do not have an entry. Messages sent from the gateway that were delivered successfully have an Activity Log entry of type 'Message'. Messages both to and from the gateway that encountered an error will have an Activity Log entry of type 'Error'.

A.3.1.7 Viewing the message content

You can view the message content if you wish. To view the content:

► Click on the entry in the Name column.

Note

For messages sent to the gateway this entry will be 'Envelope'. For messages sent from the gateway this will be 'ebxml'

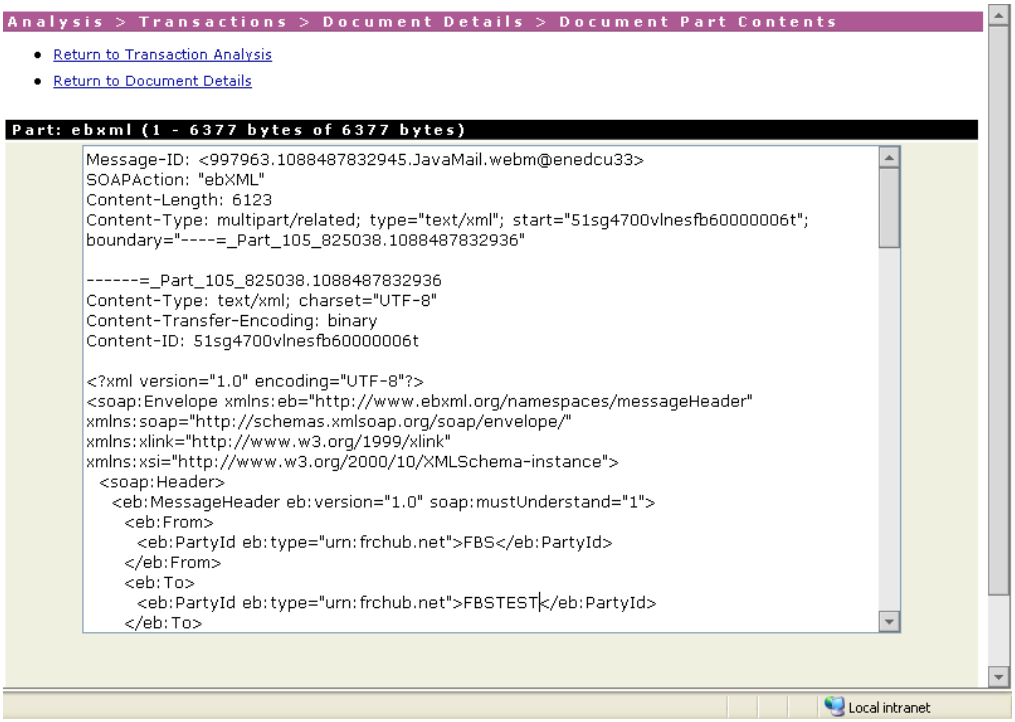


Figure 19 View document part contents window

For messages sent from the gateway the entire ebXML message, including MIME Headers and Payload, will be visible. For messages sent to the gateway only the ebXML Envelope will be visible. This is due to the current storage configuration on the hub.

A.4 System Notifications

The Responders have an interface for creating and sending specific e-mail notifications to all participants. These notifications are generally to provide information about outages or changes to a participant's gateway, which will impact other participants.

A.4.1 The Notifications Window

The Notifications Window is available on both the FBSTEST and FBS Responders.

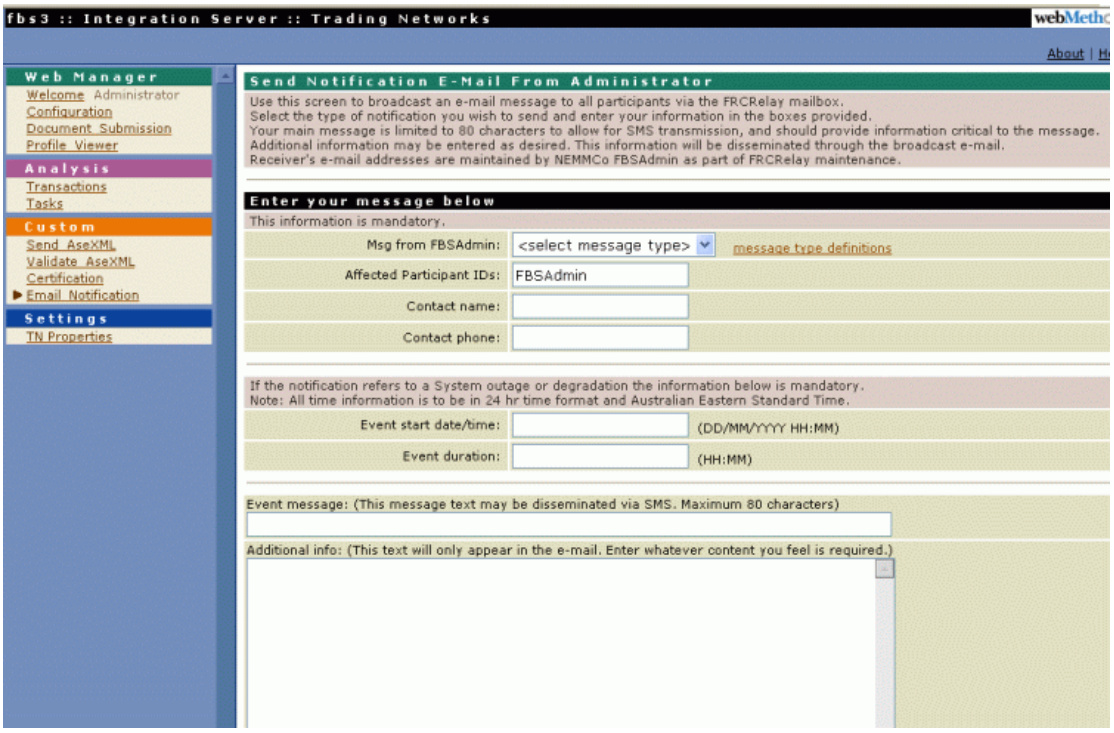
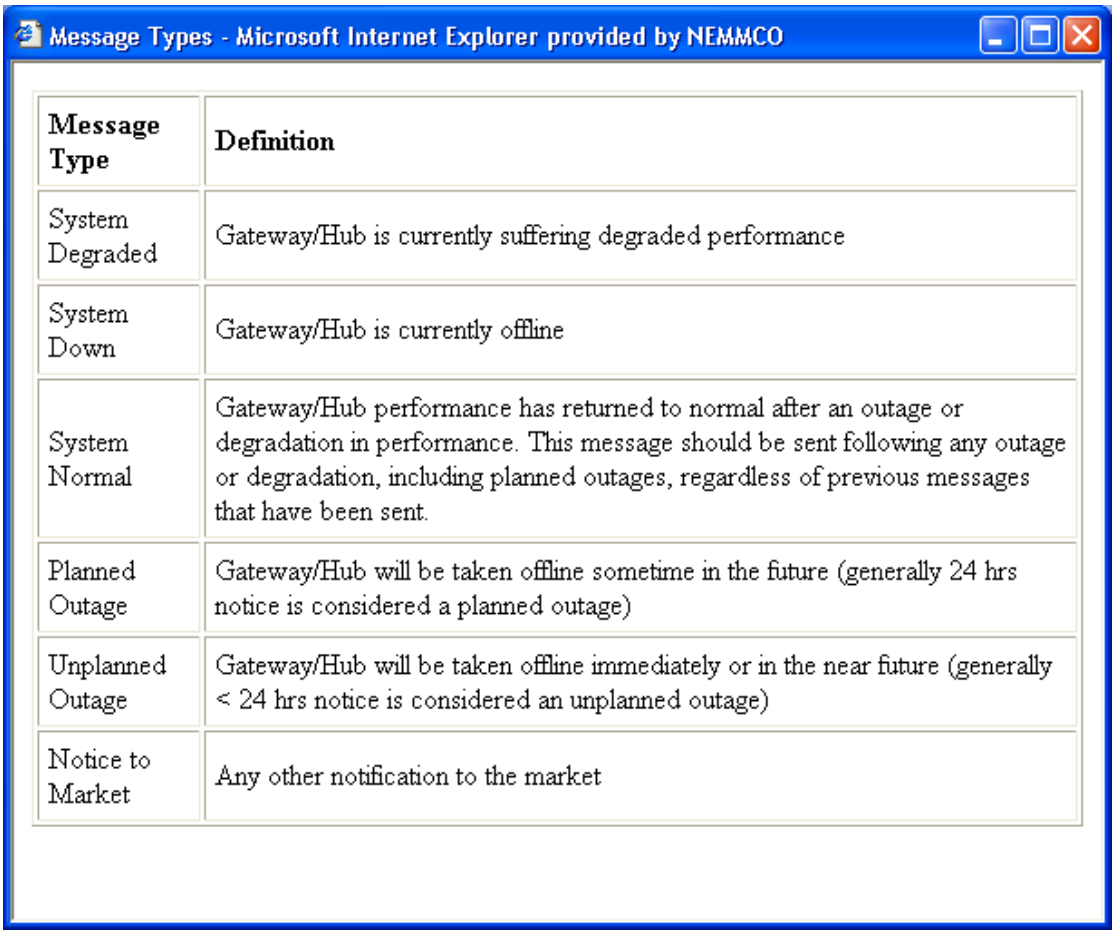

fbs3 :: Integration Server :: Trading Networks
webMeth
About
Web Manager
Welcome Administrator
Configuration
Document Submission
Profile Viewer
Analysis
Transactions
Tasks
Custom
Send AseXML
Validate AseXML
Certification
Email Notification
Settings
TN Properties
Send Notification E-Mail From Administrator
Use this screen to broadcast an e-mail message to all participants via the FRCRelay mailbox.
Select the type of notification you wish to send and enter your information in the boxes provided.
Your main message is limited to 80 characters to allow for SMS transmission, and should provide information critical to the message.
Additional information may be entered as desired. This information will be disseminated through the broadcast e-mail.
Receiver's e-mail addresses are maintained by NEMMCo FBSAdmin as part of FRCRelay maintenance.
Enter your message below
This information is mandatory.
Msg from FBSAdmin:
<select message type>
message type definitions
Affected Participant IDs:
FBSAdmin
Contact name:
Contact phone:
If the notification refers to a System outage or degradation the information below is mandatory.
Note: All time information is to be in 24 hr time format and Australian Eastern Standard Time.
Event start date/time:
(DD/MM/YYYY HH:MM)
Event duration:
(HH:MM)
Event message: (This message text may be disseminated via SMS. Maximum 80 characters)
Additional info: (This text will only appear in the e-mail. Enter whatever content you feel is required.)

Figure 20 The e-mail notifications window

A.4.1.1 To Send a Notification

1. From the Custom menu, choose Email Notification
2. Select the Message Type from the dropdown list.

Selecting the ‘message type definitions’ link will produce the following popup window to provide guidance on which message type to select:



Message Type	Definition
System Degraded	Gateway/Hub is currently suffering degraded performance
System Down	Gateway/Hub is currently offline
System Normal	Gateway/Hub performance has returned to normal after an outage or degradation in performance. This message should be sent following any outage or degradation, including planned outages, regardless of previous messages that have been sent.
Planned Outage	Gateway/Hub will be taken offline sometime in the future (generally 24 hrs notice is considered a planned outage)
Unplanned Outage	Gateway/Hub will be taken offline immediately or in the near future (generally < 24 hrs notice is considered an unplanned outage)
Notice to Market	Any other notification to the market

Tip

3. Enter the notification information in the appropriate fields as desired. The following table lists the Fields and the input required:

Field	Comments
Affected Participant IDs	All Participant IDs affected; this defaults to a single Participant ID.
Contact name	Name of the person who can provide further information if required
Contact number	Phone number of the contact
Event start date/time of incident	The date and time that the reported incident began, or will begin
Event duration	The length, or anticipated length, of the incident.
Event Message	The message to be sent. This is limited to 80 characters and should provide the critical information regarding the incident. It will be incorporated into the Subject of the e-mail.
Additional info	Any additional information regarding the incident that the participant wishes to send.

Warning

Some fields are mandatory depending on the Message Type. If a mandatory field is not populated a message will be displayed and the user prompted to correct it.

4. Click Submit

A.4.2 Secondary Notification Method

The System Notifications interface may not be available at all times. If a participant is unable to connect to FBSTEST, or FBS, to use the interface, the fall-back procedure is to send an e-mail direct to the mailbox that has been set up to forward these messages to other participants.

A.4.2.1 To send via secondary method

1. Create an e-mail in the format shown below:

```
Subject: G#FBSAdmin#Notice to Market#Start 20/02/2007 09:00 +10:00#Dur 00:00 hrs#Red Energy added
to the Prod Hub

CompanyName: FBSAdmin

AffectedParticipantIDs: FBSAdmin

EventType: Notice to Market

EventStartTime: 20/02/2007 09:00 +10:00

EventDuration: 00:00 hours

EventMessage: Red Energy added to the Prod Hub

EventAdditionalInformation: A profile has been created for Red Energy (Vic Gas Market), and
activated on the Production Hub.

ContactName: Bert Naik

ContactPhone: 03 9648 8619
```

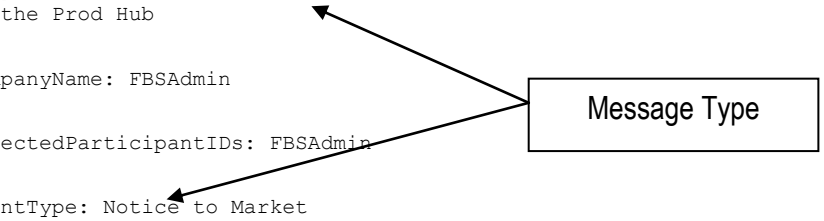


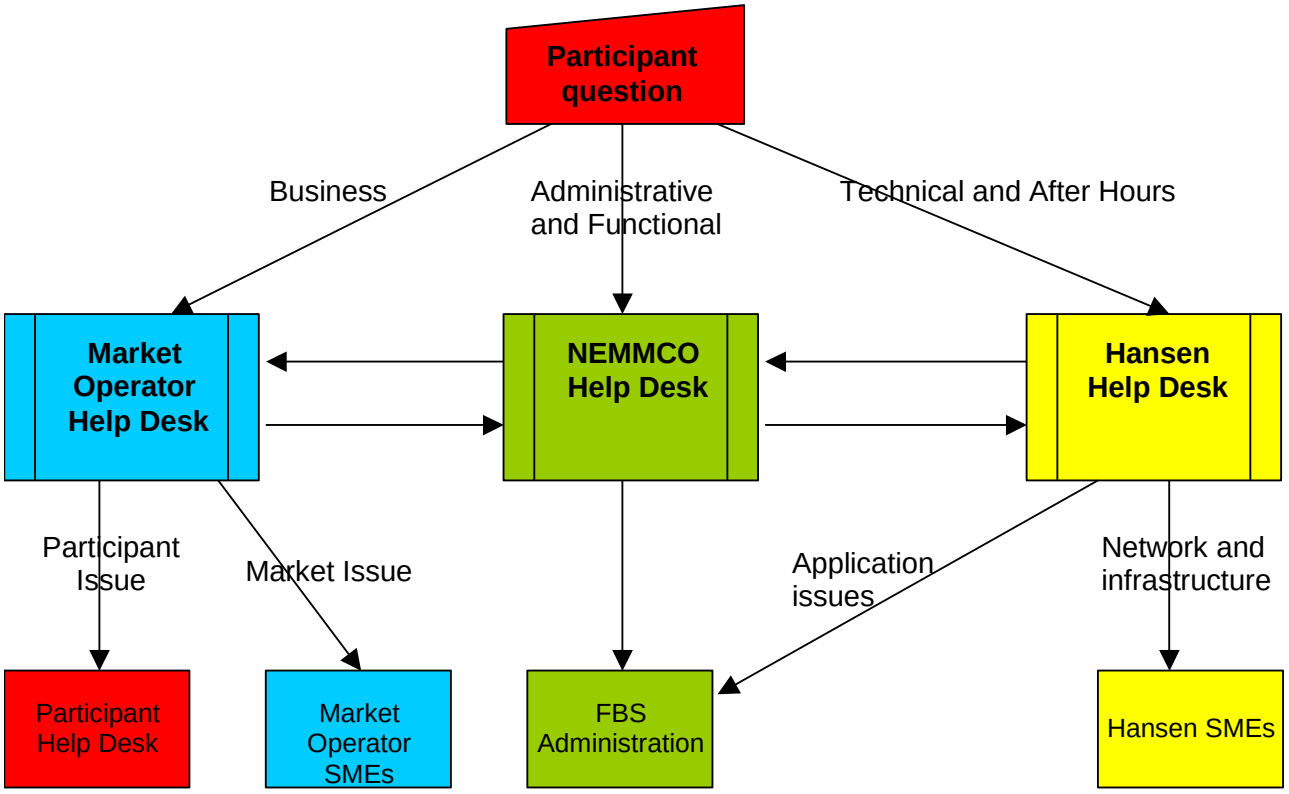
FIGURE 21 NOTIFICATION E-MAIL FORMAT

Warning

The ‘Subject’ field has been formatted to allow participants to forward it on via SMS. It must contain the critical information and not be more than 160 characters.

2. Send the e-mail to ‘frcrelay@aemo.com.au’

Appendix B Troubleshooting Guide



AEMO Gas Market Development / REMCO	AEMO Help Desk	Hansen Help Desk
These Help Desks are the first point of contact for all business (i.e. non-technical) issues. **AEMO Gas Market Development Helpdesk:** Gas.helpdesk@aemo.com.au **REMCo Helpdesk:** grmssupport@logicagmc.com.au	The AEMO Helpdesk is the first point of contact for all Hub administrative, functional and application issues and questions. **Tel:** 1300 300 295 **Fax:** (02) 8838 5061 **Email** helpdesk@aemo.com.au	The Hansen Help Desk is the first point of contact for all out-of-hours issues. During business hours, the Hansen Help Desk handles technical issues only **Tel:** 1800 625 118 **Fax:** (03) 9840 3823 **Email** helpdesk@hsntech.com

Figure 22 Troubleshooting contact guide

Appendix C Disaster Recovery Provisions

C.1 Introduction

This document outlines the major components/facilities that constitute the Gas Hub service, the impact each would have on the business in the event of a disaster and what, if any, standby services may be available.

C.2 Overview

The Hub Provider (AEMO) provides hub services from both a Primary Site, and a DR Site. The sites are interconnected, and all hub functions and data are available to participants at both sites.

Participant connectivity to both the Production and DR sites is outside of the services provided by the Hub provider, and therefore is the responsibility of each participant. As their main connection participants may select a point-to-point WAN service connecting into the Victorian Gas Industry Network (VGIN) at the hub primary site, or connection via the internet

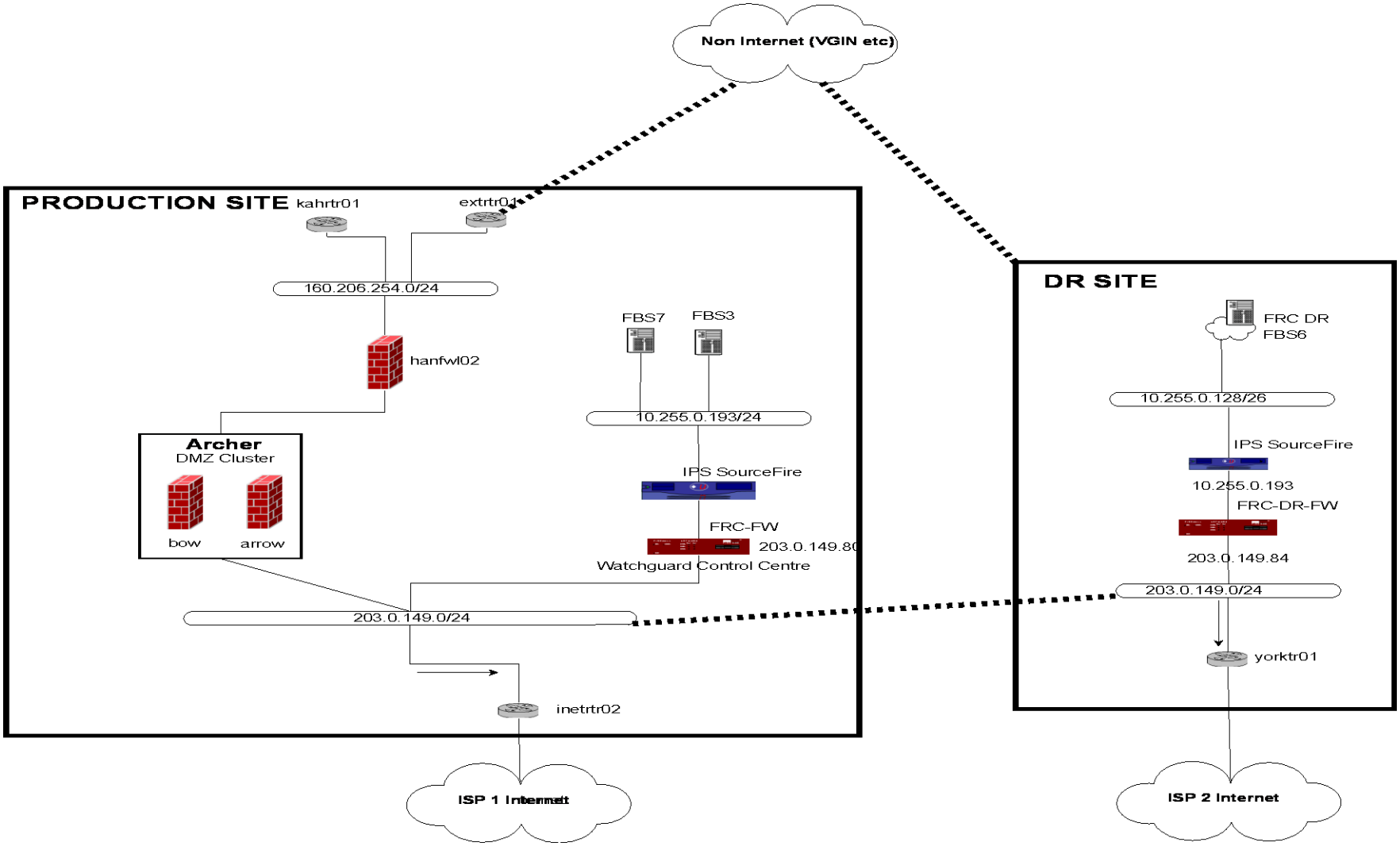


Figure 23 Network topology showing DR provisions

C.3 Disaster Scenarios

The Disaster Scenarios essentially fall under two categories depending on the extent of the disaster:

1. Where the Disaster is local to the Server and its immediate peripherals
2. Where the Disaster is more wide-spread – and could include the outage of the entire Primary site

1. The Disaster is local to the Server and its immediate peripherals

In the event that the Primary server and/or one of its immediate peripherals becomes functionally unavailable, the scenario is considered to be a Server Outage, and the Disaster Recovery is addressed by switching the processing of the messages over to the DR Server through a '***Standard'*** cutover method.

2. The Disaster is more wide-spread – and possibly includes the unavailability of the entire Primary site

In the event that the disaster covers much more than the Primary server, and/or includes the unavailability of miscellaneous infrastructural resources at the Primary site, the scenario is considered to be a Total Outage, and the Disaster Recovery is addressed by switching the processing of the messages over to the DR Server through a '***Total Outage'*** cutover method.

The table below identifies the various possibilities of component failure of the FRC Hub network, and the impact to participants and the cutover method that would be used should they fail. The table also describes any risk mitigation strategies in place for each component.

Note that, for the purposes of this section,

- Primary Production Server and the Production Hub are synonymous
- DR Server and the DR Hub are synonymous.

COMPONENT	IMPACT	MITIGATION	CUTOVER METHOD
Production Hub (FBS7)	Loss of Production Hub services	DR Hub available	***Standard***
Production Firewall (frcmel01fw01)	No access to Production Hub	No standby firewall available. 24x7, 4 hour replacement service arrangements in place.	***Standard***

COMPONENT	IMPACT	MITIGATION	CUTOVER METHOD
Production Router (Inetrtr01)	No access to Production Hub	No standby router available. 24x7, 4 hour replacement service arrangements in place.	***Total Outage***
VGIN	No access to Production Hub for participants who connect through the VGIN	Multiple components involved. Some have redundancy, some have 24x7, 4 hour replacement service arrangements in place. All VGIN participants have backup connectivity via the internet to the Production Hub	No cutover to DR. Participants would be advised to use Internet connectivity to the production Hub
VGIN	No access to Production Hub for participants who connect through the VGIN	Multiple components involved. Some have redundancy, some have 24x7, 4 hour replacement service arrangements in place. At least one of the participants has: (a) No Internet backup access to the Production Hub; (b) has a working access to the DR Hub (either via Direct link or Internet)	***Total Outage***
Internet connectivity to Primary Site	No access to Production Hub for participants who connect through the internet	Redundant internet connections to Primary Site at opposite sides of building. Alternative ISP arrangements in place.	***Total Outage***
Total loss of Primary Site	Loss of Production Hub services	DR Hub available	***Total Outage***

COMPONENT	IMPACT	MITIGATION	CUTOVER METHOD
Frame Relay Bridge to DR Site	Loss of DR traffic replication (from FBS7 to FBS6), or in the event that production has been switched over to run on FBS6 then loss of normal connectivity to Hub services.	Replication is not essential to maintain market operations.	***Total Outage***
Sybase Replicator (FBS5)	No replication of data to the backup service (FBS6).	Replication is not essential to maintain market operations. There is no additional redundancy provided for this box. The machine is backed up nightly to tape.	No cutover to DR.
Loss of any components at DR site (Hub, firewall, router, etc)	Loss of DR capability. If running on DR because of Production failure then total loss of hub services.	Loss of DR capability does not stop market operations unless Production fails. Components at DR site have 24x7, 4 hour replacement service arrangements in place.	If Primary site available then ***Standard***. Otherwise none
Loss of DR site	Loss of DR capability. If running on DR because of Production failure then total loss of hub services.	Loss of DR capability does not stop market operations unless Production fails. No backup for this facility is contracted for at this point in time. Hansen would use it's best endeavours to rectify the fault at the earliest possible convenience should an event render the facility un-useable.	If Primary site available then ***Standard***. Otherwise none

C.4 Cutover

Should the Production Hub be unavailable for more than one hour - subject to Hub Service Provider discretion - the hub services will be cutover to the DR site. The method of this cutover, as explained above, depends on the extent of the disaster, and, as outlined above, would be either a ***Standard*** cutover or a ***Total Outage*** cutover.

1. **A Standard cutover**

A Standard cutover uses the infrastructural resources (other than the Server itself) at the Primary site to route the messages to the DR site. As such, a Standard cutover expects no action from the participants.

In the Standard cutover, it is assumed that the router Inetrtr01 is accessible to all participants, and the cutover is carried out by the Hub Service Provider by changing the router configuration.

Although no action is expected from the participants as part of the cutover exercise, in certain circumstances, the participants may inadvertently get cut-off from the trading of the messages. The affected participants must contact the Hub service provider upon detection of the issue.

2. **A Total Outage cutover**

A Total Outage cutover bypasses the usage of the infrastructural resources at the Primary site. The messages to the DR site are routed independent of the Primary site. In this type of cutover, it is assumed that the router Inetrtr01 is not accessible to any of the participants.

The participants who normally use Internet for their message trading are not required to make any modifications at their gateways. The Hub Service Provider makes the necessary modifications at the Hub end to route all Internet traffic to the DR site.

However, the participants who normally access the Primary site over the VGIN are required to switch to their backup connections to access the DR Hub. These backup connections can be either:

- a (non-Internet) direct link into the DR Site facility, or
- a link over the internet.

The backup connections referred to above are also outside of the services provided by the Hub provider, and therefore are the responsibility of each participant.€